Blockchain can both enhance and undermine compliance but is not inherently at odds with EU privacy laws

Lokke Moerel and Marijn Storm

Abstract

Purpose – *To explain the authors' position that the use of blockchain technology is not incompatible with European Union privacy laws and in particular the EU General Data Protection Regulation (GDPR).*

Design/methodology/approach – *Explains the basics of blockchain technology and the GDPR, several reasons why some scholars consider BC not to be compatible with the GDPR, and why the authors believe that the GDPR will be able to regulate the use of blockchain technology.*

Findings – *The current perception is that blockchain is not compatible with EU privacy laws. The authors disagree that this is the case and explain why none of the issues identified by legal scholars and stakeholders are likely to pose issues for blockchain technology. Their conclusion is that EU privacy laws are well able to regulate also this new technology. This does however not mean that blockchain will thus be suitable for all use and deployment cases.*

Originality/value – *Practical guidance and explanation of complex issues by lawyers with extensive experience and expertise in dealing with data protection, cybersecurity, privacy, intellectual property and related issues.*

Keywords *Blockchain, Distributed ledger technology (DLT), General Data Protection Regulation (GDPR), Privacy, Data protection*

Paper type *Technical paper*

Lokke Moerel (lmoerel@mofo.com) is senior of counsel with Morrison & Foerster (Brussels) in Brussels, Belgium and professor of Global ICT Law at Tilburg University. Marijn Storm (mstorm@mofo.com) is an associate with Morrison & Foerster (Brussels) in Brussels, Belgium.

"In an almost direct clash of intentions, the GDPR has effectively banned the use of blockchain technology in Europe because of its immutable nature." – Forbes

GDPR

The EU General Data Protection Regulation or GDPR came into force on 25 May 2018. The main purposes for the European Commission (**EC**) to propose the GDPR, were the inconsistencies and fragmentation in the data protection laws of the EU Member States and the widespread lack of compliance. The GDPR now provides for one uniform law applicable to the entire EU and grants broad enforcement powers to the supervisory authorities of the Member States, including high fining powers.

The GDPR imposes strict compliance obligations on the "controller", the party who is alone or jointly responsible for the collection and use of personal data. Controller requirements include:

- Transparency, *i.e.*, informing individuals about the use of their personal data
- Limited retention, by ensuring that personal data are not stored for longer than necessary
- Data minimization, by ensuring that no more data are collected than necessary Privacy by design, *i.e.*, designing systems and solutions in a privacy-friendly manner that incorporates GDPR requirements
- Handling requests of individuals, *e.g.*, to access, correct, or delete their personal data.

Introduction

Despite the fact that blockchain technology (**BC**) [1] is not yet widely deployed, we have already seen quite some publications about the data protection issues raised by BC. Initially, these publications touted the promise of BC *increasing* privacy protection by, e.g. facilitating decentralized identity management and allowing the sharing of data with trusted third parties only (Mainelli, 2017; Zyskind *et al.*, 2015; Sater, 2017; Connor-Green, 2017; Tobin and Reed, 2017). In a second wave of publications, we saw a more in-depth discussion of the data protection issues raised by this new technology, generally concluding that *public* BC [2] features are "*on a collision course*" and "*profoundly incompatible at a conceptual level*" with the EU General Data Protection Regulation (**GDPR**) [3]. Indeed, the current conception amongst industry stakeholders is that BC is not compatible with the GDPR, resulting in a call [4] for urgent revision already right after the GDPR came into force. The concerns are fed by public statements of Jan-Philipp Albrecht (the MEP responsible for coordinating the Parliament's input for the GDPR), that BC "*probably cannot be used for the processing of personal data*" and the CNIL cautioning in its guidelines [5] that public BC may not be the most appropriate technology for processing of personal data and that priority should be given to other processing solutions that can achieve the same purpose. As the same results can currently always be achieved with another solution, this is a difficult standard to meet.

BC can both enhance and undermine compliance

As with data protection, BC may be deployed to *increase* compliance and in other cases *present* compliance issues. A key aspect of BC is an immutable ledger representing a history of transactions. As explained in the 2019 publication of George et al in this journal [6], the immutability of the BC ledger is achieved because each block of information links to the unique cryptographic identifier (or 'hash') of the previous block, thus creating a transparent and immutable chain of events.

Enhance compliance

The feature of *immutability* of the ledger can well be leveraged for compliance purposes. By using BC for identity management [7] (see for examples at the end), the effort required for a *know your customer* (KYC) check is drastically reduced, because the individual's identity is maintained on the immutable BC ledger. In a similar fashion, compliance with anti-money laundering (AML) requirements takes much less effort if all transactions are immutably recorded on the BC ledger.

Undermine compliance

An example where BC can present compliance issues is where a public BC is used for payments (e.g. Bitcoin), The Bitcoin BC, allows the transfer of Bitcoins, which can be exchanged for real-world currency, from one individual to another without anyone being aware of the identity of such individuals. In such case, AML checks are virtually impossible, which causes such currencies to be also used for money laundering and other criminal purposes.

Four issues of BC under GDPR

1. No central controller

The main issue raised by scholars [8] is that the GDPR hinges on the notion of a "controller," [9] who (alone or jointly with others) is responsible for compliance with the GDPR, in particular for implementation of *privacy-by-design* principles [10] in BC and being the addressee of requests and claims of data subjects [11]. In the current platform economy [12], it would often be possible to identify *the* entity that is the controller. With BC, there would often not be a central point of control, as *public* BC [13] dispenses with the need for intermediaries, as these are developed as open peer-to-peer systems for everyone to participate in and to effectuate trusted transactions with unknown counterparties [14]. In such set-up, it would be difficult to identify *the* controller. The authors subsequently focus on the role and function of the "nodes," [15] mentioning that a public BC is operated by all nodes in a decentralized fashion. Their conclusion is that for these BC applications, either no node would qualify as a controller (with the result that no controller could be identified at all, which cannot be the case, as the requirements of the GDPR would not apply at all), or every node would qualify as such [16]. The authors then conclude that, by lacking a better alternative, the conclusion has to be that each node qualifies as a controller and that therefore data subjects can invoke claims against each node independently [17].

2. Jurisdiction and enforcement

If each and every node qualifies as a controller, enforcement for Supervisory Authorities and data subjects would be difficult, as it is difficult to determine the exact number, location and identity of the nodes;

> As one author describes it: [18]
>
> "For the Bitcoin blockchain, there are currently approximately 11,000 nodes around the planet, of which about 1800 are in Germany and 800 in France. If one were to address each of these nodes, some of which may not be found, in a single jurisdiction this would create two sets of problems. First, a large amount of nodes would need to be contacted and compelled to comply, as opposed to a single controller in a data silo scenario. Second, this may lead to forcing all nodes to stop running the blockchain software, where GDPR rights cannot be achieved through alternative means."

3. Rights of individuals of access, correction and deletion

Nodes often only see the encrypted or hashed form of the data and are unable to make changes thereto, and therefore they cannot respond to the tasks the GDPR requires of the controller, such as providing data subjects with access to their data and to correct or delete their data where required. Due to the immutability of the BC, BC is, by definition, unable to forget, as a result of which the right to be forgotten will be impossible to enforce; [19]

4. Data accuracy and data minimization

The immutability of BC runs further contrary to the principles of data minimization and storage limitation. These principles require that controllers keep data up-to-date and do not process more data than required to fulfill the relevant purpose and also not retain such data longer than required for such use [20]. This requires that data are deleted or corrected when no longer accurate, that retention periods are defined and that the data are deleted once such retention periods expire.

A different perspective

We disagree with the analysis of the initial publications, for a host of different reasons, the main being that the authors focus on the shortcomings of the initial public (Bitcoin) BC when already many new types of *permissioned private* and *consortium* BC have been developed that significantly diverge from the original, permissionless public BC. In fact, these types of permissioned BC have been developed exactly in response to the shortcomings of public BC. The authors further consider the data processing implications of BC as if this technology constitutes in itself a data processing activity for which a controller has to be identified. Controllership is, however, decided based on a specific use or deployment of a certain technology. BC, like the internet, is a *general purpose* technology (GPT) that is subsequently deployed by actors for a certain purpose in a specific context. *Applying the question of controllership to the internet at large would pose similar data protection issues under the GDPR as identified by the authors in respect of BC. We will explain why none of these issues are currently hampering application of the GDPR to the internet and are equally unlikely to pose issues for BC applications. We see this confirmed* in a recent study of the European Parliament on BC and GDPR, concluding that BC must be examined on a case-by-case basis, rather than the technology as a whole [21].

We will explain below why none of these issues identified are currently hampering application of the GDPR to the internet and are equally unlikely to pose issues for BC applications. The conclusion is that the GDPR is also well able to regulate this new technology.

Intermediaries will not become obsolete

We consider it highly unlikely that BC will make intermediaries obsolete; rather it will replace the current intermediaries. The BC revolution is well described by the World Economic Forum (2017 report on this topic Tapscott and Tapscott, 2017), indicating that where the last decades brought us the *internet of information and the internet of things;* we are now witnessing the rise of the *internet of value*, whereby we can send money and soon any form of digitized value – from stocks and bonds to intellectual property – directly and safely between us.

As BC is about *value* (rather than just 'information'), and therefore whether someone has ownership of money, stocks, houses or not (as evidenced by the BC), the participants will insist that their stakes will be safeguarded before the BC will be trusted. The prediction is therefore that, whenever BC applications are built for evidence and transfer of value, there will always be a set of *governance rules* reflecting the terms agreed by the participants in the eco-system to regulate their relationship [22]. The first examples [23] indeed show new entities being set-up mostly as a *consortium* (often including or funded by incumbents, such as banks), which are in charge of the governance of the BC platform as well as separate entities operating a BC *application* on top of the BC platform for specific eco-systems. These BC are *permissioned*, in the sense that they implement membership rules that determine which parties have read or read/write authorization. To avoid jurisdictional and enforcement disputes, these rules will provide who the *responsible entity* is, as well as a choice of law and forum. The jurisdiction and enforcement issues raised by the authors are

therefore likely not a realistic reflection of how these issues will be encountered in practice. The controller issue is solved as in any event this central entity deciding on purposes and means of the BC platform will qualify as the controller under GDPR. The entities operating the BC application on top of the BC platform will also qualify as controllers in their own right (potentially jointly with the controller of the BC platform).

Deja vu

We here recall that early predictions in respect of the Internet foresaw similar enforcement and jurisdictional issues. Every encounter of consumers in cyberspace would raise the possibility that diverse laws would apply and multiple courts would have jurisdiction, and a myriad of court cases was predicted. Contrary to these early expectations, there have been only isolated court cases dealing with online cross-border consumer disputes. One of the explanations is that stakeholders quickly found practical workarounds in the form of contractual self-regulatory systems. Examples are the use of credit cards for online payments that bring their own dispute resolution system and the emergence of large intermediaries like eBay, which was at first just regulated by the ratings and review consumers could post, but later introduced full-fledged dispute resolution. Also, here the old intermediaries (retailers) were replaced by new intermediaries, generating again the required trust to do business. In fact, it is fair to say that there is very little happening on the Internet that is not governed by some form of contract. The use of websites is regulated by their website terms and conditions (T&Cs), online purchases are governed by purchase terms, access to the Internet is governed by the T&Cs of ISPs, App stores have their own T&Cs, search functionality is governed by the T&Cs of the provider of the search engine, etc. As happened with the Internet, it is a justified expectation that the stakeholders involved in BC will implement their own contractual self-regulatory mechanisms to ensure adequate dispute resolution.

GDPR applies to the use of a technology, not the technology itself

The authors try to determine controllership in respect of the BC technology at large, which would indeed raise the identified issues. Controllership is, however, decided based on a specific use or deployment of a certain technology. BC, like the internet, is a *general purpose technology* that is subsequently deployed by actors for a certain purpose in a specific context. None of the issues raised by the authors have hampered the development of the Internet for the simple reason that controllership is not decided based on the technical level of operation of the relevant technology, but is based on who deploys this technology for a certain purpose. For example, a website owner uses the Internet to offer its website. It is the website owner who qualifies as the controller in respect of the processing of any personal data via the website and not the operator of the technical infrastructure.

GDPR does not impose requirements on designers of technology

GDPR includes an obligation for the controller to set up data processing functions on the basis of *privacy-by-design* (Article 25 GDPR). GDPR does not impose this requirement on providers of software and infrastructure that are used to process personal data. As a consequence, individual controllers need to expressly instruct each of their technology suppliers to provide software and infrastructure that incorporate privacy-by-design in order to meet their controller obligations.

Although this indirect manner of regulating seems inefficient, the reality is that for technology developers it is often difficult to foresee all possible deployments of their technology. As a consequence, it is difficult to implement all requirements into their product from the outset. It is often in the feedback loop of the users, customers or society at large when the technology is deployed in practice that the design issues become apparent and

are addressed. Too-strict upfront design requirements (in the form of standards) may even hamper innovation, and it may even lead to "widespread adoption of inferior technology," (as explained in a report of the World Economic Forum.(World Economic Forum, 2017)] In the words of Brian Behlendorf (CEO of the Linux Foundation):

> "*The space is still so young that the desire for standards, while well-placed, runs the risk of hardening projects that have just come out of the lab'' and ''we need to avoid making serious architectural decisions that first become legacy and then become a hindrance.*"

GDPR is, just as its predecessor, technology agnostic (see Recital 15 of the GDPR) in the sense that it provides for general data protection principles and requirements but does not prescribe any technology or technical manner how these principles and requirements should be implemented. As BC is an emerging technology still in its infancy, GDPR works exactly as it is intended, challenging developers to think of creative ways of how to develop the technology in such a manner that the impact on the privacy of individuals can be mitigated and basic principles of GDPR can be complied with. That this may take some development cycles to be achieved is fully understood. The conclusion of the authors – that GDPR is thus unable to embrace this new technology – is missing the point that GDPR is intended to provide guidance on how to develop new technology in the first place. Below we will discuss how the transparency and immutability issues raised by BC can be addressed by implementing innovative privacy-by-design measures.

What are the real data protection issues?

The fact that BC, both public and private, is inherently transparent and immutable may clash with data minimization principles and may make it impossible to respond to rights of individuals to have their data corrected or deleted. BC is further by definition unable to forget, as a result of which the right to be forgotten will be impossible to enforce. The transparency and immutability issues can, to a large extent, be addressed by implementing innovative privacy-by-design measures (see for examples below, such as, limiting the storage on the BC ledger, and pruning the BC ledger.). Noteworthy is that these innovations are not necessarily triggered by privacy considerations, but mostly out of efficiency considerations.

In its most basic form, a BC can be used to store plain text information on the ledger, which information can be accessed by those who have read rights. Storing all information on the BC takes up a large amount of space on the BC and takes a lot of energy both to run and cool the machines. Block space can be saved by separating (segregating) the signature ('witness') information from the transaction data (the 'payload'), so the network can increase the transactions processed. These measures may well also to a certain extent mitigate transparency issues.

The immutability of the BC further does not sit well with, for example, **smart contracts** in more complex transactions (as contracts often have to be amended for unforeseen circumstances), with **technological malfunction**, including in case of interference by hackers; and more in general with **human messiness** (known to lose their BC private key). Solving these issues will require solving the immutability of the BC, which may well also solve the issue of being able to respond to requests of individuals for deletion and the right to be forgotten.

Immutability is not always an issue

As a side note we mention that the immutability of BC is not always an issue. For certain applications (in particular in case of public registries), immutability is actually a requirement. Illustrative here is the judgment of the European Court of Justice in the *Manni* case [24]. The plaintiff (Mr. Manni) requested deletion of his personal information from the Italian public

company register where information on his prior bankruptcy was recorded. He argued that this record in the company register was widely reused by data brokers, as a result whereof his reputation was prejudiced having a detrimental effect on his new business. The ECJ balanced the public interest in the legal certainty in trade and transparency of business information in the company register with the fundamental right to data protection and concluded that, in this case, the interference with the rights to data protection was not disproportionate taking into account the limited amount of personal information held in the company register.

In line with the above ruling, registering limited personal data in a BC for public registers like land ownership, trademark ownership, company registers, may therefore well be justified. The above case entails that a balancing of interests should be made for each BC application. For other use cases, the balancing test may well conclude that BC will not be suitable as the impact on data protection will be disproportionate. An example of the latter would be if BC would be applied to provide air passengers with expedited access through the airport, meanwhile also recording all money spent in shops and restaurants at airports, subsequent transport and accommodations on the BC for purposes of a loyalty program. Using BC for the commercial loyalty program would likely be disproportionate.

Five privacy-by-design options

1. Limit ledger storage

The original Bitcoin BC stores the full ledger on every node, making it impossible to make changes to prior blocks and thus providing for an indisputable ledger for all prior transactions. However, this also means that the personal data included on the ledger is shared with a large number of nodes (Bitcoin has approximately 9,500 nodes). Storing so many instances of personal data is at odds with the data minimization principle of the GDPR, which requires access to personal data to be limited to the fewest possible recipients.

A privacy-by-design solution is to no longer store the entire ledger on all nodes. In most Bitcoin instances, the validity of a new block is verified by a consensus mechanism. This means that the creator of the block provides a unique hash of the information. The nodes make the same mathematical equations and, if the outcome of this hash is the same, the block is verified. This requires the nodes to have access to the information included on the block. However, the nodes would still be able to fulfil their verification function if they would delete the information after verification. This will increase the confidentiality of the personal data included on the block and, at the same time, has economic advantages. If each node has to store a full copy of the ledger, a large amount of storage capacity is required that, in turn, requires a large investment in data storage and uses a lot of energy. Therefore, storing the ledger in one (or a few) instances rather than on every node has both privacy and economic advantages.

2. Pruning

Most BC applications store all transactions since the start of the chain, dating back to the 'genesis block', which means that all transactions on this BC are stored infinitely (and, as set out above, are sometimes stored on all nodes). Storing data infinitely is, by definition, at odds with the GDPR's data minimization requirement but also brings ever-increasing storage requirements. For example, during a stress test, the size of the BC of an Ethereum client increased to 40 gigabytes in the first three months of the test.

A privacy-by-design solution to this storage issue is pruning, which enables the node to verify a new block without processing historical transactions by having the node download as much block-headers as it can and determine which header is on the end of the longest

chain. Starting from this header on the longest chain, the node goes back 100 blocks to verify that the chain matches up. Because this verification process removes the need for retaining the entire chain history for verification purposes, this allows for the removal of unused blocks, which drastically lowers the required storage and implements data minimization into the BC. To ensure that no data is lost, the unused blocks can be stored in one or more archive nodes, which store all data just in case the rest of the network needs them in the future, but the 'active' nodes no longer have to process these archived blocks.

3. Privacy-friendly consensus

A privacy-by-design solution for the infinite storage issue is the concept of non-interactive zero-knowledge proof, which makes it possible to verify the correctness of a computation, e.g., a hash, without having to execute the computation or even learning what was executed. For example, the proposed currency Zerocoin (MIERS *et al.*, 2013) works as follows. When a coin is purchased, a serial number is attributed to the coin, which can only be revealed using a random number. Using these two numbers, a user can generate a zero-knowledge proof for the fact that the user knows both the serial number and the random number. This zero-knowledge proof can then be verified by the network without having access to the coin's serial number or the random number.

The potential use of zero-knowledge proof is not limited to the transfer of coins using BC but can be used to verify any computation without having access to the underlying information. This enables nodes to reach consensus on a new block, without accessing the information on that block, and thus without sharing the personal data included on that block with the nodes.

4. Editable BC

A more radical approach that solves a number of BC data protection issues is the editable BC, for which Accenture has been awarded a patent (Accenture, 2016). The editable BC uses the 'chameleon' hash function, which allows for changing the underlying information without changing the outcome of the hash function. This allows for changes to the underlying information of which the hash is already included on the BC, which makes it possible to correct (human) error or intentional (fraudulent) inaccuracies on the BC. This would allow for the execution of individuals' rights under the GDPR, e.g., to correction and to be forgotten.

Solving the immutability of BC comes at a price. To a large extent, the trust in BC application relies on the network's consensus on the content of a block and the immutability of the content thereafter. When removing this immutability, other measures should be implemented to retain (or gain) sufficient trust in the BC application for individuals and organizations to use it as a record of their transactions. The trust in a BC application could be retained if, for example, only a single trusted entity can make these changes, similar to the fact that only governments can make certain changes to governmental public registries. A different solution could be to implement a very strict change management procedure, which could include a consensus mechanism that verifies the legitimacy of a change. In any event, changes will have to be strictly logged to ensure that changes can always be reviewed and explained in the future.

5. BC self-sovereign' identity management

The well-known use cases of BC are mostly focused on administering transactions, but BC can also be deployed for *privacy enhancing* purposes, for example by facilitating 'self-sovereign' identity management.

In the offline world, an individual's identity is mostly established by verifying an individual's driver's license or passport. The strength of this system follows from a trusted central governmental authority that provides these proofs of identity. However, because the online world does not follow the national boundaries of the offline world, it is difficult to appoint such trusted centralized authority for an online proof of identity. By now, there are many initiatives to provide individuals with a digital identity. An example of how BC can be deployed for online identify management is the initiative of Microsoft and Accenture providing a BC based solution designed to allow individuals with direct control over who has access to their personal data. Rather than that all service providers each collect and store the personal data required for providing services to an individual, the personal data are stored off-chain and the system only calls on these data when the individual grants access, whereby access can be limited both in scope and in time. For example, when an individual needs to prove his or her identity when renting a car, the access to the identifying information can be limited to what is necessary to provide this proof and for a short period of time only.

Decentralized identity management has a number of benefits. From a privacy point of view, it enables individuals to take back control over their digital identity, coined the 'self-sovereign identity'. Currently, many individuals are, for example, not aware of the use of their digital identity and personal data, e.g. for advertising purposes. By using a decentralized identity system, individuals would be able to decide who to give access to which information for which period of time. A single decentralized identity system also has economic benefits. Right now, a large number of companies are storing similar information about the same individuals. A decentralized identity management system makes this duplicated storage obsolete and ensures that companies have access to up-to-date information on an individual, insofar as the individual wants the company to have such access.

Editor's note

This article provides a summary of an academic article authored by Lokke Moerel first published in European Review of Private Law, 6–2019.

Notes

1. In this article we will use the narrower term of BC rather than distributed ledger technology (DLT), for reasons of readability, acknowledging that there are other forms of DLT to which this article would equally apply.
2. There are broadly three categories of BC: private, consortium and public BC. ***Private BC*** is maintained by a limited number of network nodes belonging to an organization. Read rights can be granted to computers that belong to the network, or could also be granted to selected external computers. ***Consortium BC*** is generally used by a number of different organizations belonging to a consortium, and involves nodes of the relevant organizations only; here, also, read rights can be controlled. ***Public BC*** may involve any computer that opts to be a network node and can read/write the BC. Examples of the latter are Bitcoin or Ethereum. Another distinction is between permissioned and permissionless BC: permissioned BC is open to pre-defined subjects only and permissionless BC allows all those with the necessary technical capacity to take part. Private and consortium BC are mostly (but not necessarily) permissioned BC, and public BC is mostly permissionless.
3. Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation), eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:TOC).
4. See D. MEYER, *IAPP* (2018), for a number of quotes from stakeholders voicing concerns that BC is incompatible with the GDPR, that the GDPR is therefore already out of date and therefore already needs urgent revision; see in similar vein (and with similar quotes) also Ward (2018); and Avan-Nomayo (2018).

5. CNIL "Solutions for a responsible use of the blockchain in the context of personal data" (2018), p. 5: "*While appropriate safeguards for a transfer outside the EU may be used in a permissioned blockchain, such as standard contractual clauses, binding corporate rules, codes of conduct or even certification mechanisms, the CNIL observes that these safeguards are harder to implement in a public blockchain, given that the data controller has no real control over the location of miners.*", available at: www.cnil.fr/sites/default/files/atoms/files/blockchain_en.pdf
6. R. GEORGE ET AL, *Journal of Investment Compliance*, Vol. 20, No. 1, 2019, pp. 17-21.
7. B. KOMMADI, *Blockchain – An Elixir for Anti-Money Laundering?*, available at https://doi.org/10.1002/9781119551973.ch39
8. The authors all also discuss whether the data stored on the BC qualifies as personal data under the GDPR but generally conclude that the GDPR applies to the processing of personal data stored on the BC also if pseudonymized, encrypted or hashed. This is a correct conclusion, as these measures all concern measures that mitigate the impact on the privacy of individuals rather than fully anonymize the personal data that would bring these data outside the scope of applicability of the GDPR, see Article 29 Working Party, Opinion 04/2014 on Anonymisation Techniques, 0829/14/EN, at 20. For reasons of space, I will refrain from discussing these issues here. See for the conclusion that GDPR applies, M. FINCK, *MPI Paper* (2017), p. 16 and M. BERBERICH; M. STEINER, *EDPLR* (2016), p. 424; and Wirth and Kolain (2018).
9. The entity that, alone or jointly with others, determines the purposes and means of the data processing (Art. 4 GDPR).
10. Article 25 GDPR.
11. See for rights of data subjects Articles 12-22 GDPR.
12. M. FINCK, *MPI Paper* (2017), at 6 describes it as follows: "the GDPR was fashioned for a world where data is centrally collected, stored and processed, [while] blockchains decentralize each of these processes." BC would offer a record keeping function that "dispenses with the need for an intermediary," which is "in sharp contrast with the current data economy, characterized by economic centralization in the form of 'platform power."
13. See for description of the various categories of BC.
14. M. FINCK, *MPI Paper* (2017), p. 6 and M. BERBERICH and M. STEINER, *EDPLR* (2016), p. 422.
15. BC is a distributed peer-to-peer ledger stored on every node of the system. If a new transaction is effected, the nodes verify the legitimacy of the effected transaction and, for some BC applications, provide decentral storage for the BC's ledger. Any device with an internet connection can be used as a node but, due to the processing and storage requirements, mostly computers are used as nodes. The node willingly contributes (a part of) its processing or storage abilities to the BC network. Alternatively, some forms of malware transform the device of an unsuspecting user into a node, sapping its processing or storage abilities.
16. M. FINCK, *MPI Paper* (2017), p. 16 and M. BERBERICH and M. STEINER, *EDPLR* (2016), p. 423.
17. See M. FINCK, *MPI Paper* (2017) at p. 17 for an explanation why it is justified that each node qualifies as a controller: "nodes are indeed not subject to external instructions, autonomously decide whether to join the chain, and pursue their own objectives [...] it appears that the Regulation's legal obligations would rest on each node, meaning that data subjects can invoke claims via-à-vis each node independently;" see also M. BERBERICH and M. STEINER, *EDPLR* (2016), p. 424; C. WIRTH and M. KOLAIN, *Reports of the European Society for Socially Embedded Technologies* (2018), p. 5, under reference to Martini and Weinzierl (2017), at p. 1251-1259.
18. M. FINCK, *MPI Paper* (2017), p. 17.
19. M. FINCK, *MPI Paper* (2017), p. 20-24 and M. BERBERICH and M. STEINER, *EDPLR* (2016), p. 426.
20. M. FINCK, *MPI Paper* (2017), p. 20 and M. BERBERICH and M. STEINER, *EDPLR* (2016), p. 424-425.
21. EUROPEAN PARLIAMENT, *Blockchain and the General Data Protection Regulation*, p. 101: "*Indeed, the key takeaway from this study should be that it is impossible to state that blockchains are, as a whole, either completely compliant or incompliant with the GDPR. Rather, while numerous important points of tension have been highlighted and ultimately each concrete use case needs to be examined on the basis of a detailed case-by-case analysis.*", available at: europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf.

22. Tapscott and Tapscott (2017), p. 9: "It illustrates the profound differences between managing information creation versus value creation activities. The latter require deep negotiation, contractual and jurisdictional understandings, and the ongoing stewardship of application-level ecosystems." This may well be in the form of 'membership rules' governing the decentralized organization, see de Filippi and Wright (2015), at p. 31.

23. See for an overview of the top 10 cryptocurrencies and a discussion of the set-up and governance of a number of these as well as subsequent governance challenges, D. TAPSCOTT and A. TAPSCOTT, *WEF Report* 2017 at pp. 1017. See also at p. 25 where the challenge is discussed that "powerful encumbrants will usurp domains" by being the largest investors in BC ventures.

24. ECJ March 9, 2017, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v Salvatore Manni,* ECLI:EU:C:2017:197.

References

Accenture (2016), "Editing the uneditable blockchain, why distributed ledger technology must adapt to an imperfect world", available at: newsroom.accenture.com/content/1101/files/Cross-FSBC.pdf

Avan-Nomayo, O. (2018), "Parity forced to shut down ICO passport service (picops) due to GDPR", available at: bitcoinist.com/parity-forced-to-shut-down-picops-due-to-gdpr/

Connor-Green, D. (2017), "Blockchain in healthcare data", *Intellectual Property and Technology Law Journal*, Vol. 21, p. 93.

de Filippi, P. and Wright, A. (2015), "Decentralized blockchain technology and the rise of lex cryptographia", *Socials Sciences Research Network* (March 10).

Mainelli, M. (2017), "Blockchain will help Us prove our identities in a digital world", *Harvard Business Review*, available at: hbr.org/2017/03/blockchain-will-help-us-prove-our-identities-in-a-digital-world

Martini, M. and Weinzierl, Q. (2017), "Die Blockchain-Technologie und das recht auf vergessenwerden", *Neue Zeitschrift für Verwaltungsrecht (NVwZ)*.

Miers, I., Garman, C., Greend, M. and Rubin, A.D. (2013), "Zerocoin: anonymous distributed E-Cash from bitcoin", *IEEE*, doi: 10.1109/SP.2013.34.

Sater, S. (2017), "Blockchain and the European union's general data protection regulation: a chance to harmonize international data flows", *Tulane University*, available at: papers.ssrn.com/sol3/papers.cfm?abstract_id=3080987

Tapscott, D. and Tapscott, A. (2017), "Realizing the potential of blockchain".

Tobin, A. and Reed, D. (2017), "The inevitable rise of Self-Sovereign identity", *Sovrin Foundation*, Vol. 1(March 28), available at: sovrin.org/wp-content/uploads/2017/06frhe-Inevitable-Rise-of-Self-Sovereign-Jdentity.pdf

Ward, S. (2018), "Blockchain to clash with new EU privacy law", available at: www.bestvpn.com/privacy-news/blockchain-clash-new-eu-privacy-law

Wirth, C. and Kolain, M. (2018), "Privacy by BlockChain design: a blockhain-enabled GDPR-compliant approach for handling personal data", *Reports of the European Society for Socially Embedded Technologies*, doi: 10.18420/blockchain2018_03, pp. 4-5.

World Economic Forum (2017), "Realizing the potential of blockchain", available at: www3.weforum.org/docs/WEF_Realizing_Potential_Blockchain.pdf

Zyskind, G., Nathan, O. and Pentland, A. (2015), "Decentralizing privacy: using blockchain to protect personal data", *IEEE CS Security and Privacy Workshops*, available at: ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7163223

Corresponding author

Lokke Moerel can be contacted at: lmoerel@mofo.com